Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

July 26 - Aug 01, 2022

Report Summary:

- **New Threat Detection Added** – 6 (8220 Gang, Loli Stealer Malware, BokBot Malware, Kimsuky APT, VPNFilter and CVE-2021-41773)
- **New IDPS Rules Created**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**
- **Total Counts by Observable Type**

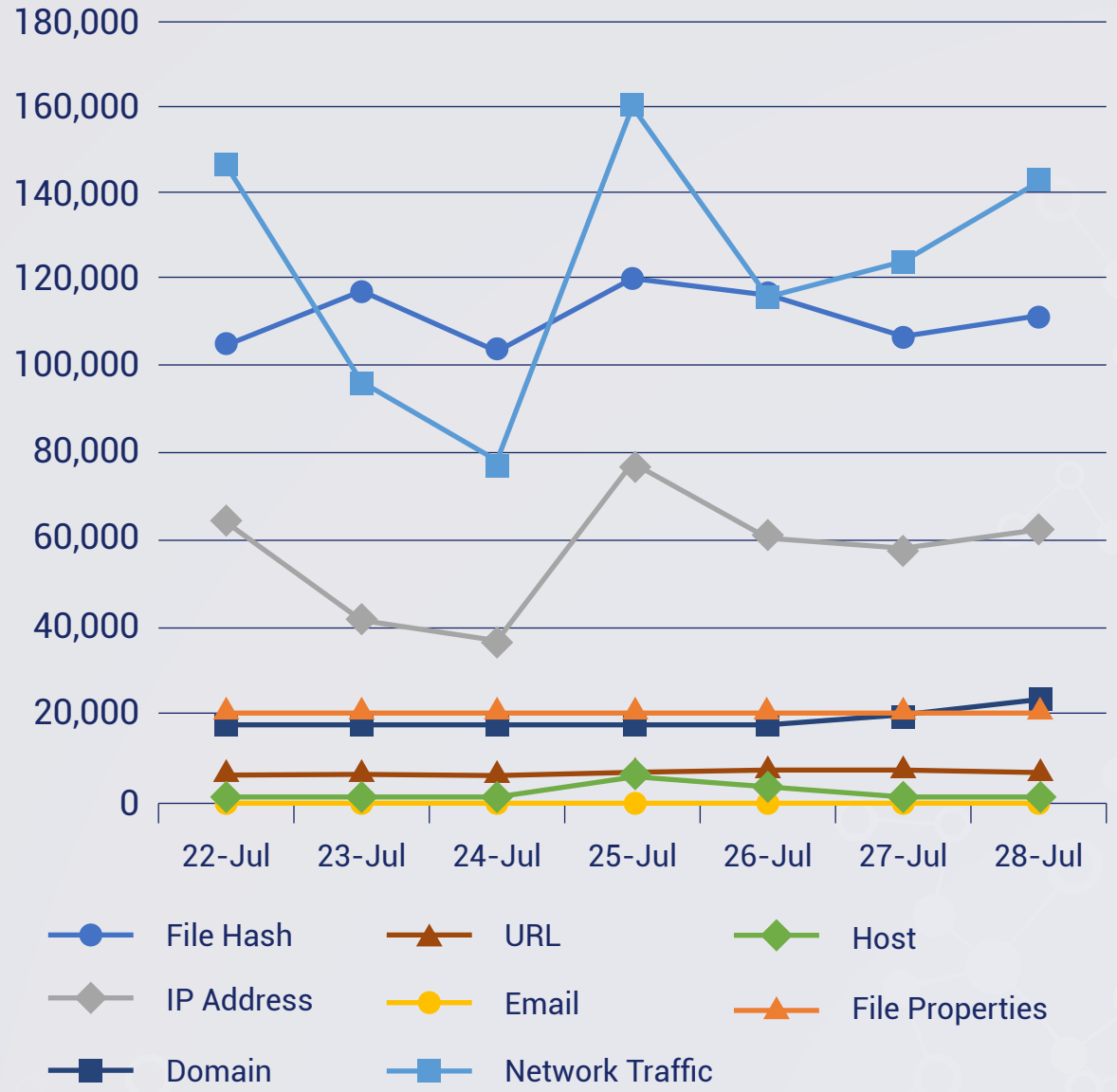
IDPS Rules Created (Week Ending 01/08/2022):

12

Overall Weekly Observables Count:

2,369,884

Daily Submissions by Observable Type:



Newly Detected Threats Added

The following threats were added to Crystal Eye XDR this week:

1. 8220 Gang (Malware)

Microsoft has warned against a malware dubbed as 8220 gang targeting Linux systems and installing crypto-mining malware. Researchers named the attacker 8220 gang and spotted notable updates to the malware campaign, which includes a new variant of crypto miner, and an IRC bot. Microsoft has disclosed the recent attacks of the 8220 gang, in which they were found exploiting a critical bug affecting Atlassian Confluence Server and Data Center. The recent campaign targets i686 and x86_64 Linux systems. It employs RCE exploits for CVE-2019-2725 (Oracle WebLogic) and CVE-2022-26134 (Atlassian Confluence Server and Data Center) for initial access.

Rules Created: 03
Rule Set Type: Balanced – IDS: Alert – IPS: Alert
Class Type: Trojan Activity
Kill Chain: Initial Access T1189 - Execution T1059 - Persistence - Command and Control T1102

2. Loli Stealer (Malware)

The Loli Stealer Malware packed with UPX & written in Go programming language also dubbed as Golang Stealer recently detected by Malwarebytes as Trojan.CryptoStealer.Go. As its behaviour, the malware calls WindowsAPI for example, PIN tracers. The malware then calls to the Yandex browser, which is popular mainly in Russia. Next, it searches for the desktop and copies all files to a folder created in %APPDATA%. The malware finally copies all files, compresses them all and sends them to its command-and-Control server.

Rules Created: 2
Rule Set Type: Balanced
Class Type: Trojan Activity
Kill Chain: Execution T1204- Discovery T1087-Collection T1119- Command and Control T1071

3. BokBot (Malware)

BokBot, also known as IcedID, was initially known as a banking trojan that steals credentials from a victim's online banking session. Once installed on a computer, it finds credentials from the browser and initiates fraudulent bank transactions. A recent campaign from the threat group TA551 was observed to push BokBot from their activities.

Red Piranha has deployed rules that will detect the initial download of this password-protected archive. The domains have also been identified and shall be rejected once domain requests are observed from machine endpoints.

Rules Created: 3
Rule Set Type: Security – IDS: Alert – IPS: Reject
Class Type: Trojan-activity
Kill Chain: Initial Access T1566 - Execution T1059 – Credential Access T1539 - Command and Control T1102

4. Kimsuky APT (Threat Actor)

Kimsuky APT, a North Korean threat group known to conduct government cyber espionage operations, has been recently discovered targeting military base maintenance providers. A common tactic for Kimsuky APT is to lure their targets with phishing emails resembling a notice from the government ministry department. This will include a malicious document that appears as a sign-up form; once executed, it will immediately contact its command-and-control server for further instructions.

Red Piranha has deployed new rules that will detect the initial domain requests for recently discovered Kimsuky APT-related sites. The traffic shall be rejected once observed from machine endpoints.

Rules Created: 1
Rule Set Type: Balanced – IDS: Alert – IPS: Reject
Class Type: Trojan-activity
Kill Chain: Initial Access T1566 - Execution T1204 - Command and Control T1102

5. VPNFilter (Malware)

The VPNFilter malware is a multi-stage, modular platform with versatile capabilities to support both intelligence-collection and destructive cyber-attack operations. The stage 1 malware persists through a reboot, which sets it apart from most other malware that targets internet-of-things devices because malware normally does not survive a reboot of the device. The main purpose of stage 1 is to gain a persistent foothold and enable the deployment of the stage 2 malware. Stage 1 utilizes multiple redundant command and control (C2) mechanisms to discover the IP address of the current stage 2 deployment server, making this malware extremely robust and capable of dealing with unpredictable C2 infrastructure changes.

The stage 2 malware, which does not persist through a reboot, possesses capabilities that we have come to expect in a workhorse intelligence-collection platform, such as file collection, command execution, data exfiltration and device management. However, some versions of stage 2 also possess a self-destruct capability that overwrites a critical portion of the device's firmware and reboots the device, rendering it unusable. Based on the actor's demonstrated knowledge of these devices, and the existing capability in some stage 2 versions, we assess with high confidence that the actor could deploy this self-destruct command to most devices that it controls, regardless of whether the command is built into the stage 2 malware.

In addition, there are multiple stage 3 modules that serve as plugins for the stage 2 malware. These plugins provide stage 2 with additional functionality. there are two known plugin modules: a packet sniffer for collecting traffic that passes through the device, including theft of website credentials and monitoring of Modbus SCADA protocols, and a communications module that allows stage 2 to communicate over Tor.

Rules Created: 1
Rule Set Type: Balanced – IDS: Alert – IPS: Alert
Class Type: Malware
Kill Chain: Initial Access T1566 - Execution T1204 - Command and Control T1102

6. CVE-2021-41773

A flaw was found in a change made to path normalization in Apache HTTP Server 2.4.49. An attacker could use a path traversal attack to map URLs to files outside the directories configured by Alias-like directives. If files outside of these directories are not protected by the usual default configuration "require all denied", these requests can succeed. If CGI scripts are also enabled for these aliased paths, this could allow for remote code execution. This issue is known to be exploited in the wild. This issue only affects Apache 2.4.49 and not earlier versions. The fix in Apache HTTP Server 2.4.50 was found to be incomplete.

Rules Created: 2
Rule Set Type: Balanced – IDS: Alert – IPS: Alert
Class Type: RCE
Kill Chain: Initial Access: T1133

Total Counts by Observable Type:

The table below shows the total counts of observables we've been collecting for the last four months, the last four weeks, and the total since February 2017.

	Date	File Hash	IP Address	Domain	URL	Email	Network Traffic	Host	File Properties	Total
Month	Apr 2022	4,124,667	1,837,957	396,073	637,235	592	3,514,384	371,365	563,861	11,446,134
	May 2022	4,029,272	1,798,537	476,808	448,583	168	3,194,022	179,741	590,291	10,717,422
	Jun 2022	4,798,835	2,138,981	548,365	473,164	735	3,645,625	115,609	585,476	12,306,790
	Jul 2022	3,292,459	1,463,827	484,583	212,732	17	2,955,718	68,835	551,316	9,029,487
Week	7/1-7/7	943,452	438,030	126,350	62,360	0	810,711	23,358	135,432	2,539,693
	7/8-7/14	751,304	314,639	113,855	54,821	14	710,598	15,133	139,544	2,099,908
	7/15-7/21	817,762	312,021	117,953	46,922	0	576,167	11,451	137,726	2,020,002
	7/22-7/28	779,941	399,137	126,425	48,629	3	858,242	18,893	138,614	2,369,884
Total	Since Feb 2017	154,801,123	36,825,172	20,219,962	15,829,282	198,904	30,096,704	2,822,491	3,365,864	264,159,502